



# FortiClient (Windows App) - User Guide

VERSION 1.0

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



February 23, 2018

FortiClient 1.0 (Windows App) User Guide

04-100-370210-20180223

# TABLE OF CONTENTS

<b>Change Log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
FortiClient (Windows App) features	5
SSL DNS server and DNS suffix	5
Supported platforms	5
<b>Initial Configuration</b>	<b>7</b>
Download the installer	7
Running FortiClient (Windows App)	8
To add a VPN connection:	8
To connect to a VPN connection:	11
To disconnect from a VPN connection:	13
To edit or remove a VPN connection:	13

# Change Log

Date	Change Description
2016-05-02	Initial release of 1.0.0.
2016-09-06	Updated "Supported server address formats" on page 10.
2016-09-07	Added an <i>Ignore server certificate</i> note to "To connect to a VPN connection:" on page 11.
2016-09-12	Initial release of 1.0.1.
2017-03-08	Added "SSL DNS server and DNS suffix" on page 5.
2018-02-23	Release of single merged document for 1.0 releases.

# Introduction

FortiClient is an all-in-one comprehensive endpoint security solution that extends the power of Fortinet's Advanced Threat Protection (ATP) to end user devices. As the endpoint is the ultimate destination for malware that is seeking credentials, network access, and sensitive information, ensuring that your endpoint security combines strong prevention with detection and mitigation is critical.

This guide describes how to install and set up FortiClient (Windows App) for the first time.

## FortiClient (Windows App) features

Feature	Description
SSL VPN (Tunnel Mode)	SSL VPN in Tunnel Mode supports the following: <ul style="list-style-type: none"><li>• Full tunnel &amp; split tunnel (IP and subnet based)</li><li>• SSL realm, custom DNS server, DNS suffix</li><li>• Username &amp; password authentication</li><li>• PKI user with a personal certificate, FortiToken &amp; Client Certificate</li></ul>

## SSL DNS server and DNS suffix

Example to configure SSL DNS server and DNS suffix by using FortiOS:

```
config vpn ssl settings
    set dns-suffix
    "domain1.com;domain2.com;domain3.com;domain4.com;domain5.com;domain6.com;domain7.com;domain8.com"
    set dns-server1 10.10.10.10
    set dns-server2 10.10.10.11

config vpn ssl web portal
    edit "full-access"
        set dns-server1 10.10.10.10
        set dns-server2 10.10.10.11
        set split-tunneling enable
```

## Supported platforms

FortiClient (Windows App) supports the following operating systems:

- Windows 10
- Windows 10 Mobile

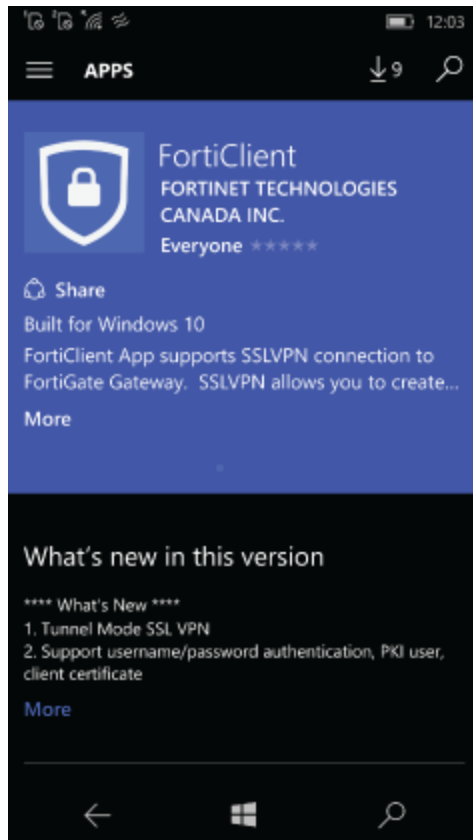


FortiClient (Windows App) requires FortiOS 5.2.4 or higher.

---

# Initial Configuration

## Download the installer



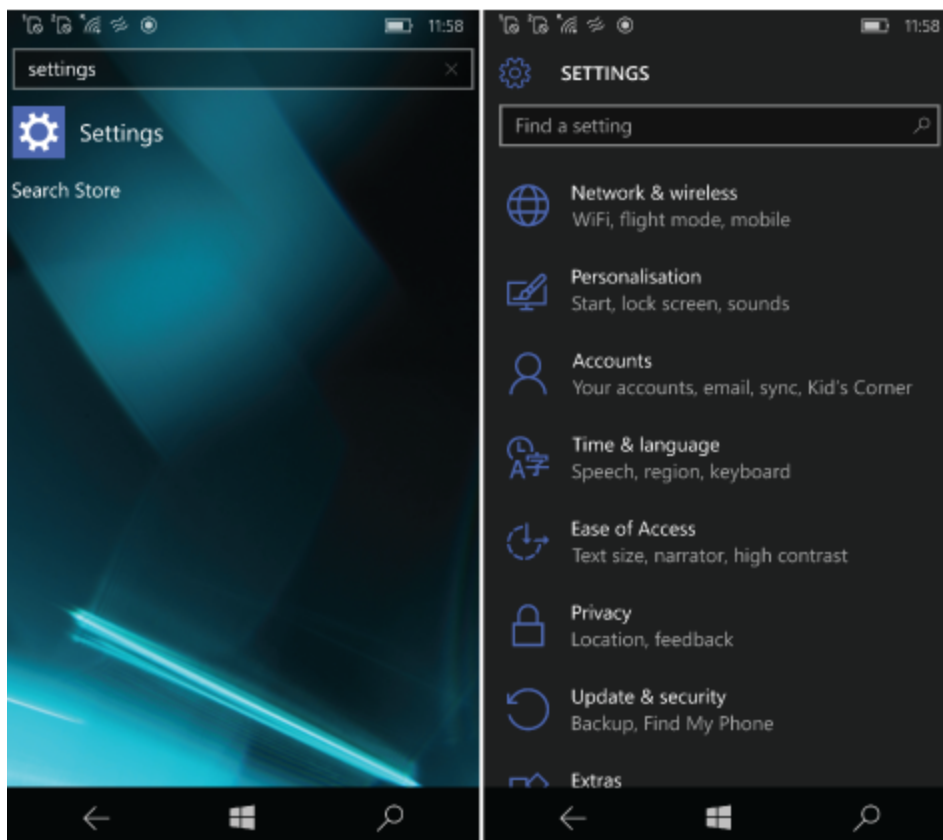
FortiClient (Windows App) is available for download from the:

- Microsoft Store: <https://www.microsoft.com>

## Running FortiClient (Windows App)

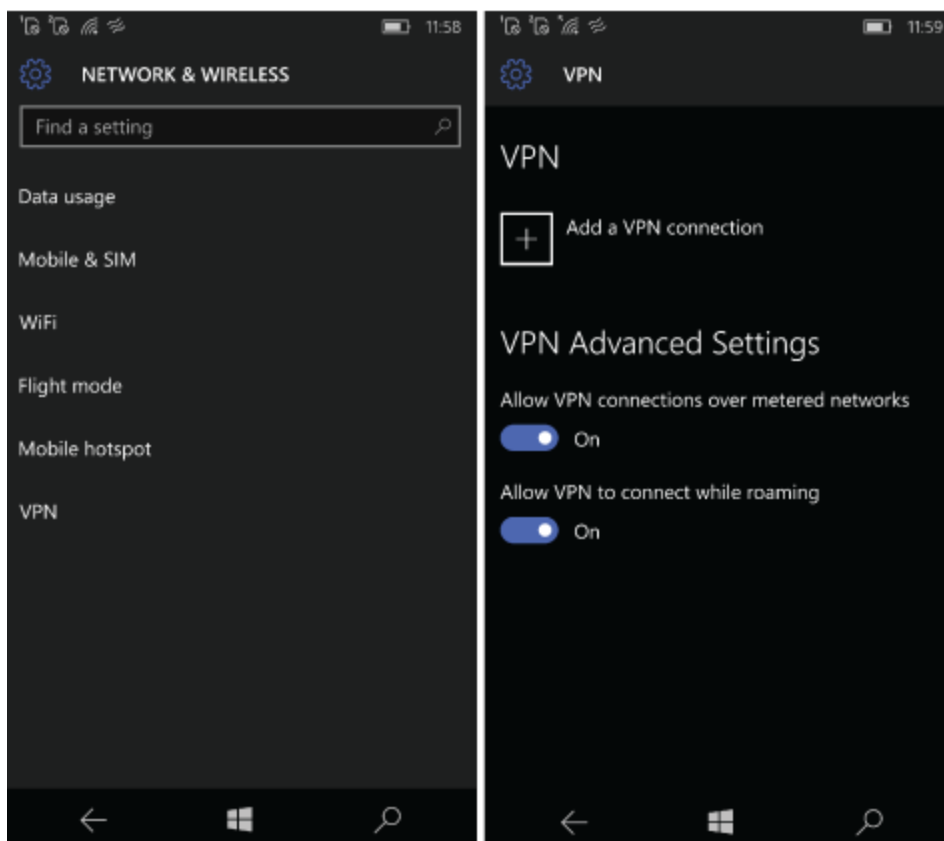
### To add a VPN connection:

1. Go to *Settings*.

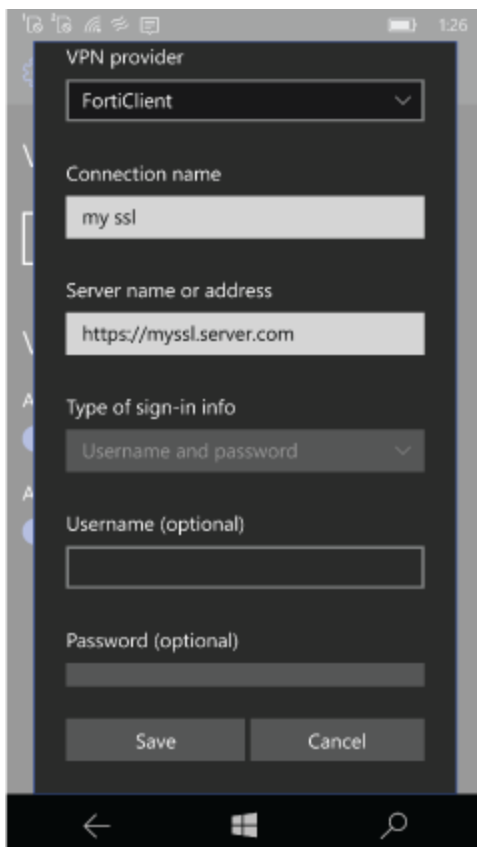


2. Tap *Network & Wireless*.
3. Tap *VPN*.





4. Tap *Add a VPN connection*.
5. Configure the following:



<b>VPN Provider</b>	Select FortiClient.
<b>Connection Name</b>	Enter a name for the connection.
<b>Server name or address</b>	Enter the server.  A list of supported server address formats is provided below.
<b>Type of sign-in info</b>	Leave as is. Do not enter any information.
<b>Username (optional)</b>	Leave as is. Do not enter any information.
<b>Password (optional)</b>	Leave as is. Do not enter any information.

7. Tap Save.

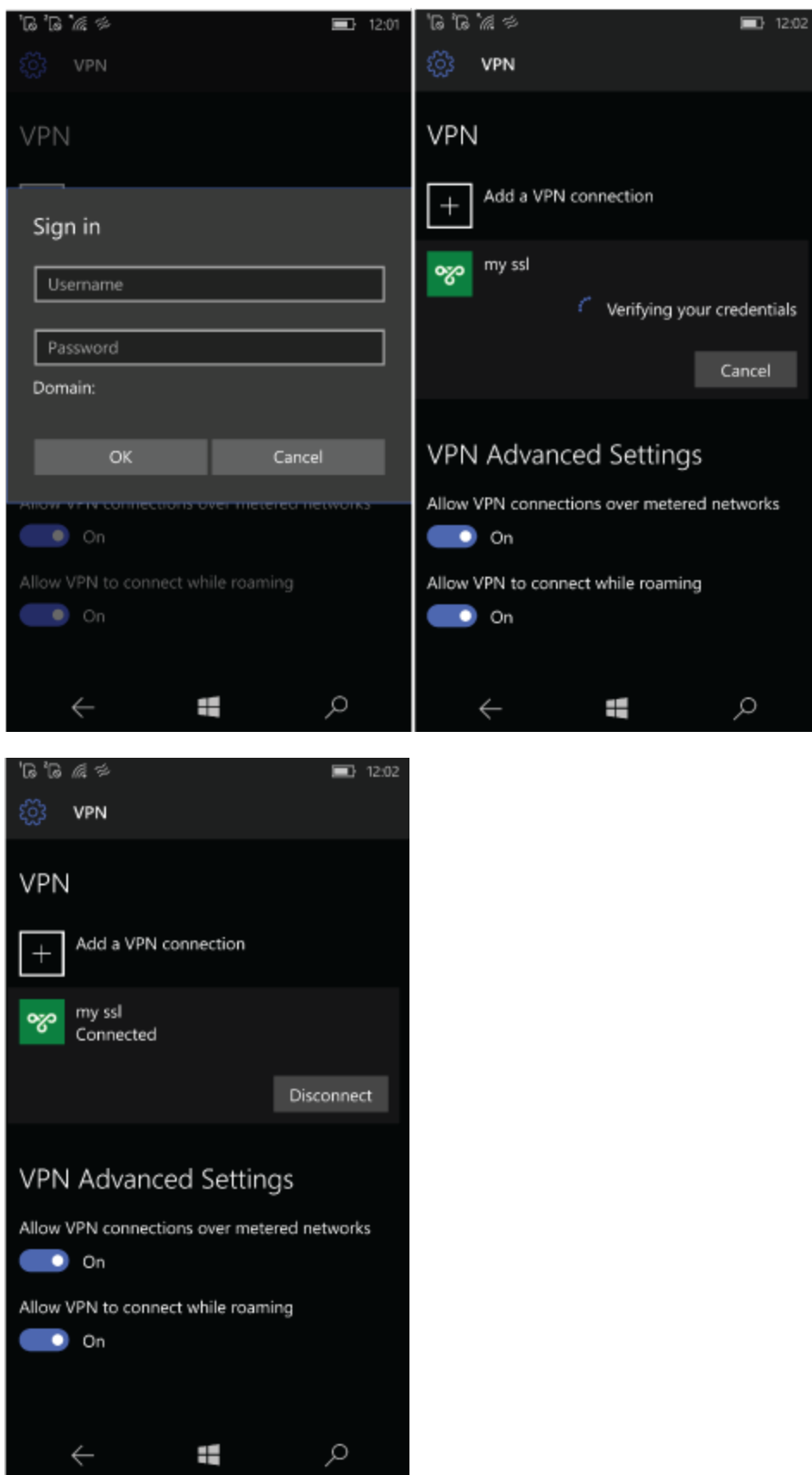
### Supported server address formats

<b>To use default port 443</b>	<ul style="list-style-type: none"><li>• <a href="https://vpn.server.address.com/">https://vpn.server.address.com/</a></li></ul>
<b>To use a custom port (e.g. 10443)</b>	<ul style="list-style-type: none"><li>• <a href="https://vpn.server.address.com:10443">https://vpn.server.address.com:10443</a></li></ul>

<b>To use a realm (e.g. realm-name)</b>	<ul style="list-style-type: none"> <li>• <a href="https://vpn.server.address.com/realmname">https://vpn.server.address.com/realmname</a></li> </ul>
<b>A combination of customer port and realm</b>	<ul style="list-style-type: none"> <li>• <a href="https://vpn.server.address.com:10443/realmname">https://vpn.server.address.com:10443/realmname</a></li> </ul>
<b>Ignore server certificate error</b>	<ul style="list-style-type: none"> <li>• <a href="https://vpn.server.address.com/?ignore-certificate-errors=1">https://vpn.server.address.com/?ignore-certificate-errors=1</a></li> <li>• <a href="https://vpn.server.address.com/?ice=1">https://vpn.server.address.com/?ice=1</a></li> <li>• <a href="https://vpn.server.address.com/?ice">https://vpn.server.address.com/?ice</a></li> </ul>
<b>Enable pop-up to select the client certificate</b>	<ul style="list-style-type: none"> <li>• <a href="https://vpn.server.address.com/?cert=">https://vpn.server.address.com/?cert=</a></li> </ul>
<b>Pre-configure a client certificate</b>	<ul style="list-style-type: none"> <li>• <a href="https://vpn.server.address.com/?cert=client">https://vpn.server.address.com/?cert=client</a> Where client is a substring of the certificate subject.</li> </ul>
<b>Use a PKI user (certificate user)</b>	<ul style="list-style-type: none"> <li>• <a href="https://vpn.server.address.com/?cert=&amp;no-username-password=1">https://vpn.server.address.com/?cert=&amp;no-username-password=1</a></li> <li>• <a href="https://vpn.server.address.com/?cert=&amp;nup=1">https://vpn.server.address.com/?cert=&amp;nup=1</a></li> <li>• <a href="https://vpn.server.address.com/?cert=&amp;nup">https://vpn.server.address.com/?cert=&amp;nup</a></li> </ul>

### To connect to a VPN connection:

1. Tap a *VPN connection*.
2. Tap *Connect*.
3. Enter your *Username* and *Password*.



4. Tap *OK*.



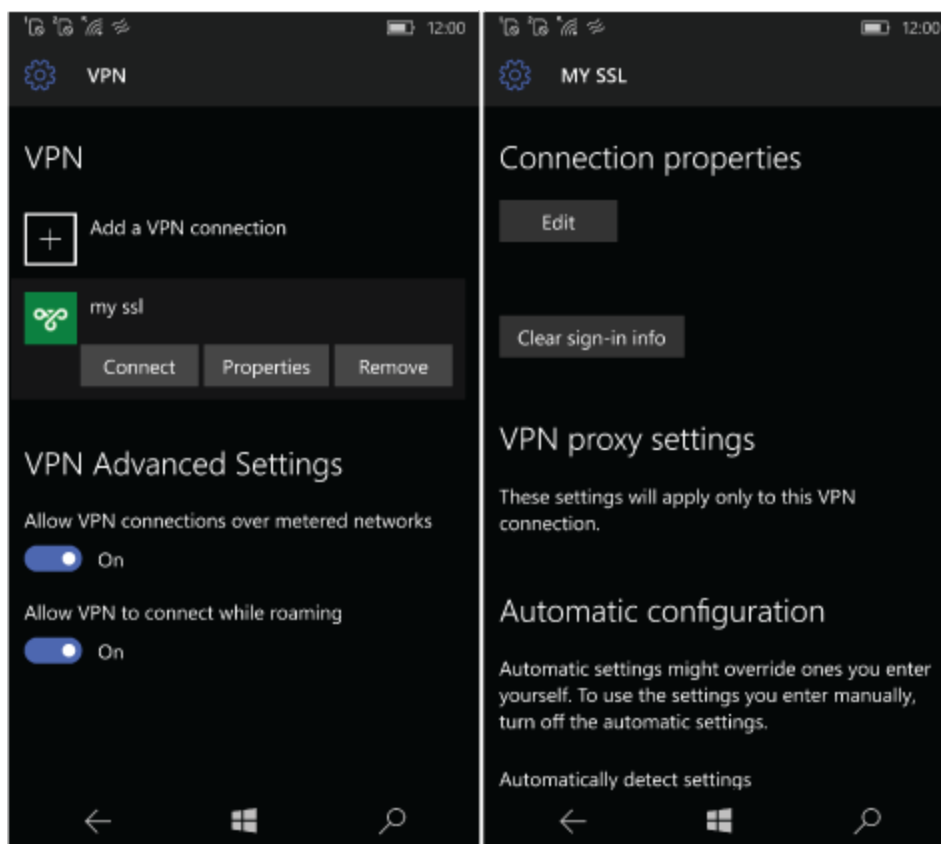
A certificate error can cause the *Sign In* screen to continuously display even when you use the correct username and password to connect to the network by using a VPN connection. You can instruct the VPN configuration to ignore the certificate error by using the *Ignore server certificate* feature. See the [Supported Server Address Formats](#) section.

### To disconnect from a VPN connection:

1. Select the VPN connection.
2. Tap *Disconnect* to disable the VPN connection.

### To edit or remove a VPN connection:

1. Select a VPN connection.



2. Tap *Properties/Remove*.
3. Tap *OK* to save the settings.



**FORTINET®**

*High Performance Network Security*



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.